UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

CISCO SYSTEMS, INC. and CISCO TECHNOLOGY, INC.,	:	
Plaintiffs,	:	19 Civ. _____
-against-	:	
SHENZHEN TIANHENG NETWORKS CO; GEZHI PHOTONICS TECHNOLOGY CO., LTD.; SHENZHEN SOURCELIGHT TECHNOLOGY CO.; HU JIANGBING; LI PAN; DONG DAOSHUN; WANG WEI; and DARIOCOM,	:	**FILED *EX PARTE* AND UNDER SEAL PURSUANT TO 15 U.S.C. § 1116**
Defendants.	:	

PLAINTIFFS' EMERGENCY MOTION FOR ORDER TO SHOW CAUSE AND MEMORANDUM OF LAW IN SUPPORT OF ORDER TO SHOW CAUSE FOR TEMPORARY RESTRAINING ORDER, ASSET FREEZE ORDER, EXPEDITED DISCOVERY, ORDER PERMITTING ALTERNATIVE SERVICE OF PROCESS, AND PRELIMINARY INJUNCTION

TABLE OF CONTENTS

Page

TABLE OF CONTENTS
(continued)

Page

TABLE OF AUTHORITIES

Page(s)

Cases

TABLE OF AUTHORITIES
(continued)

Page(s)

TABLE OF AUTHORITIES
(continued)

Page(s)

TABLE OF AUTHORITIES
(continued)

Page(s)

TABLE OF AUTHORITIES
(continued)

Page(s)

TABLE OF AUTHORITIES
(continued)

Page(s)

Statutes

Rules

Other Authorities

Plaintiffs Cisco Systems, Inc. and Cisco Technology, Inc. (together, "Cisco") submit this memorandum of law in support of their application for an Order to Show Cause seeking a temporary restraining order and a preliminary injunction to prevent Defendants, all of whom are China-based online sellers, from continuing to distribute and sell counterfeit Cisco transceivers in the United States. Cisco also seeks an order freezing Defendants' assets and disabling their online presence, as well as expedited discovery so that Cisco can identify all channels through which Defendants are distributing counterfeit Cisco products and locate all of Defendants' unlawfully gained assets. In addition, Cisco seeks an order authorizing alternative service of process. The requested relief has frequently been granted by federal courts, including the Eastern District of New York, on the *ex parte* application of counterfeiting victims.

INTRODUCTION

Cisco brings this action in an urgent effort to remove dangerous counterfeit transceivers from the U.S. market. Cisco transceivers are the leading products in their class and are used in countless public and private computer networks, including those operated by the U.S. government, the U.S. military, hospitals, transportation systems, and virtually everyone else. In short, Cisco transceivers are part of the backbone of the United States' communications and informational infrastructure, including access to the internet. The counterfeit transceivers sold by Defendants pose a serious risk to that national infrastructure, and it is difficult to overstate the potential for harm that creates in countless aspects of governmental, military, commercial, and personal life. To take a salient example, the U.S. military's networks are built on Cisco transceivers, and according to the trial testimony of a representative of the U.S. Marine Corps, the risk of using substandard counterfeit Cisco products could not be higher: "Marines could die."

The Defendants in this action are Chinese companies that Cisco recently discovered publicly offering suspect Cisco transceivers online to U.S. consumers. Through its investigators, Cisco made a series of test purchases of purported Cisco transceivers that the Defendants sold and shipped into this District. Cisco carefully tested and analyzed the transceivers sold by the Defendants, and confirmed that every transceiver received from every Defendant was counterfeit. That conclusion was confirmed by Cisco's manufacturing partners, who also tested and analyzed the Defendants' transceivers. On the outside, the Defendants' transceivers have product labels that bear a counterfeit Cisco logo and provide false, inaccurate product numbers and security serial numbers. Internally, the counterfeit transceivers are cobbled together from unapproved, non-genuine components, and do not meet Cisco's design and build standards. Moreover, each counterfeit transceiver was loaded with read-only memory that falsely identified "CISCO" as the vendor and contained incorrect attributes that do not reflect the attributes of a genuine Cisco transceiver.

In order to immediately remove these dangerous counterfeit Cisco products from the U.S. market, Cisco brings this anti-counterfeiting action for trademark infringement pursuant to the Lanham Act (15 U.S.C. §§ 1114 & 1125) and New York State law. Consistent with the relief sought by other victims in anti-counterfeiting actions brought in New York federal court and elsewhere, Cisco seeks four types of relief. The relief sought is aimed both at putting an immediate stop to Defendants' ability to sell the counterfeits into the United States, as well giving effective notice to these overseas Defendants and securing their participation in this litigation First, Cisco seeks a temporary restraining order and preliminary injunction preventing Defendants from selling Cisco-branded products. Second, in order to preserve its ability to recoup the profits that Defendants earned from the sale of dangerous counterfeits Cisco products

and maintain the status quo, Cisco seeks an *ex parte* order freezing the assets of Defendants, disabling Defendants' seller identifications and domain names and transferring them to Cisco's care, and shutting down Defendants' ability to sell any Cisco products online and ship them to U.S. consumers. Third, Cisco seeks an order granting limited expedited discovery so that it may rapidly locate and remove from the market any other counterfeits that are being sold in the United States. Fourth, Cisco requests the authority to effect service of process through alternative means, including by email.

STATEMENT OF FACTS

A. Cisco's Transceiver Products

Cisco has been selling networking equipment, including pluggable transceiver modules ("Cisco transceivers") since 1984. *See* Declaration of Charles Williams, dated November 19, 2019 ("Williams Decl.") ¶ 4. Cisco is the nation's (and the world's) leader in developing, implementing, and providing the technologies behind networking, communications, and information technology products and services, and ships over 10 million transceivers per year. *Id.* ¶¶ 4, 10.

Cisco transceivers are electronic devices that use fiber optical technology to transmit and receive data. *See* Declaration of Michael Heidecker, dated November 19, 2019 ("Heidecker Decl.") ¶ 8. In basic terms, a transceiver encodes and decodes data by converting an electrical signal into light pulses, which are sent through a fiber optic cable, where they are received at the other end and converted back into an electrical signal. *Id.* A network's performance is contingent on transceivers. *See* Williams Decl. ¶ 11. Cisco transceivers provided the vital connection. *Id.* The quality of the networks in the United States and around the world is dependent on authentic Cisco transceivers. *Id.*

Cisco markets and sells a wide range of transceivers that vary in size, price, and functionality. *See* Heidecker Decl. ¶ 8. Each Cisco transceiver is designed to meet and exceed industry standards for quality, reliability, safety, and performance. *Id.* A wide variety of American industries rely on the performance of high-quality Cisco transceivers to perform critical and life-essential applications. *See* Williams Decl. ¶ 12. This includes the U.S. government, U.S. military, and hospitals, among many others. *Id.* These governmental and healthcare infrastructures are built on Cisco products to maintain the security of data storage and ensure the integrity of data transfer and communications. *Id.*

All authentic Cisco transceivers are manufactured by heavily-vetted and carefully controlled and monitored third-party vendors called original equipment manufacturers ("OEMs"). *See* Heidecker Decl. ¶ 9. Most of Cisco's transceivers are manufactured and distributed by one of three OEMs: Methode Electronics, Inc.; FINISAR Corporation; and Foxconn Interconnect Technology, Ltd. *See id.* Each of these OEMs utilize specialized equipment and heavily-tested processes to produce consistent, high-performing products on which consumers can rely. *Id.*

Cisco requires its OEMs to follow strict quality and control standards that govern the entire product lifecycle of each transceiver, from its design, components, and manufacture to distribution and post-sale support. *Id.* ¶ 10. Each OEM facility undergoes reliability demonstration testing to expose any potential undiscovered defects that may be induced by the manufacturing process. *Id.* After the OEM is approved for manufacture and distribution, Cisco conducts ongoing reliability testing and performs quarterly business reviews that comprehensively examine the OEM's practices and procedures and identify areas for improvement. *Id.* Cisco also performs regular, stringent audits on each OEM, which must

maintain detailed production data records for each serialized product and logs of product movement throughout the supply chain. *Id.* These records give Cisco the ability to monitor each transceiver's distribution and to support customers via serial number traceability. *Id.* Cisco uses these controls and others to safeguard its reputation for safety, reliability, and quality. *Id.*

B. Counterfeit Cisco Transceivers Are Dangerous

Defendants' transceivers are confusingly similar to Cisco's authentic product; bear counterfeit and confusingly similar imitations of the CISCO Marks; and are not manufactured by Cisco or any party associated or affiliated with, or authorized, licensed, or approved of by Cisco. *See id.* ¶¶ 16, 19-21, 24-26, 29-32, 35-39; Williams Decl. ¶¶ 15-16, 19-22. In short, Defendants deceive consumers by delivering to them low-quality counterfeit products instead of high-quality genuine Cisco products. *Id*

The counterfeit transceivers sold by the Defendants pose very significant dangers. Because counterfeits have non-approved components, they may not function properly or at all, and may not function correctly in combination with authentic Cisco products and components. *Id.* Nor are they updated with the latest Cisco software. *See* Williams Decl. ¶ 21. This leaves users exposed to security and intrusion vulnerabilities. *Id.*

Data integrity is critical to the industries and businesses that utilize Cisco transceivers. The importance of data integrity is particularly strong for government, military, financial services, healthcare, energy and utilities, and transportation networks, all of which need to reliably and securely transmit and receive data. *Id.* ¶ 22. Counterfeit transceivers jeopardize the data integrity of all of these networks and the people they serve. *Id.* While consumers and industries believe their network is protected, the counterfeit transceivers leave dangerous gaps in network security. *Id.*

The risk posed by the counterfeit transceivers includes physical harm. Cisco transceivers use different transmitter laser technologies, which require extensive eye-safety testing and manufacturing calibration in order to ensure user's physical safety. *Id.* Counterfeit transceivers are not subjected to this testing. *Id.* Moreover, a poorly designed transceiver, such as the counterfeits sold by Defendants, can emit excessive electromagnetic energy that will interfere with adjacent equipment. *Id.* This can be detrimental in any environment where sensitive electronic equipment is present, including in a military command, hospital, or data center. *Id.*

Counterfeit transceivers also put lives in jeopardy. The U.S. military, including the Marine Corps, utilizes the Cisco-based classified network for all of its battle operations, including sharing intelligence, convoy operations, troop movements, air operations, call for fire, and medevacs. In a federal criminal action brought by the U.S. government against a counterfeiter of Cisco networking hardware, *United States v. Ehab Ashoor*, No. H-09-CR-307 (S.D. Tex.), U.S. Marines Staff Sergeant Lee Chieffalo testified before a jury about the U.S. military's extensive use of Cisco products: "[t]he Marine Corps' network infrastructure is solely Cisco equipment," and "the equipment that Cisco uses has proprietary protocols and software on them that operates only with other Cisco gear." Williams Decl. ¶ 13 & Ex. 2. He explained that Cisco gear is "built to specifications that [the Marine Corps] use[s] for reliability and environmental hardness." *Id.* According to Staff Sergeant Chieffalo, the risk of using substandard counterfeit Cisco products could not be higher: "Marines could die." *Id.* The Department of Homeland Security has reached the same conclusion: "These cases [of counterfeit Cisco networking products] involve greedy businessmen hocking counterfeit and substandard hardware to any buyer—whether it could affect the health and safety of others in a hospital setting or the security of our troops on the battlefield…. They pose a triple threat to our

nation by stealing from our economy, threatening U.S. jobs and potentially putting the safety of our citizens at risk." *Id.* ¶ 14 & Ex. 3.

C. Trademarks Used on Cisco Transceivers

Cisco is the owner of the following well-established famous and registered trademarks (together, the "CISCO Marks") that appear on the genuine Cisco products:

- "CISCO" (REG. NOS. 1,542,339; 2,498,746; 3,709,076; 3,978,294; 3,985,844; 3,990,147; 4,005,670)
-  (Reg. Nos. 3,759,451)

See Williams Decl. ¶¶ 4-9 & Ex. 1. Cisco has used, and is currently using, the CISCO Marks continuously and exclusively in commerce, including in connection with its sale of Cisco transceivers, and plans to continue such use in the future. *Id.*

Cisco has invested heavily in the CISCO brand. *Id.* Cisco prominently displays the CISCO Marks in its advertising and promotional materials. *Id.* As a result of extensive promotion and widespread sales, the CISCO Marks are widely recognized and have become well known to the public and synonymous with reliable, high-quality networking hardware products. *Id.* Cisco has spent, and continues to spend, millions of dollars marketing and promoting in interstate commerce these products in connection with the CISCO Marks. *Id.*

Cisco has engaged and continues to engage in activities designed to promote Cisco products and the business and goodwill associated with its trademarks, and to expand the use and reputation of its trademarks, logos, and property throughout the United States and world. *Id.* Due to Cisco's longtime use of and investment in the CISCO Marks and the quality of Cisco's products, the Cisco brand has built up a tremendous amount of consumer goodwill. *Id.* The CISCO Marks are famous and symbolize this goodwill; they are invaluable assets to Cisco. *Id.*

D. Discovery and Testing of Counterfeit Cisco Transceivers

The success of the Cisco brand has attracted criminal counterfeiters who sell fake Cisco products to reap an illegal profit. To combat this counterfeiting, Cisco investigates, among other things, suspicious listings on online marketplaces. *See* Heidecker Decl. ¶ 15. Through such an investigation Cisco identified and arranged for a private investigator to purchase suspect Cisco transceivers from each Defendant. *See id.*; Declaration of Carlo Vogel, dated Nov. 18, 2019 ("Vogel Decl.") ¶ 4.

Cisco maintains three lab facilities that are dedicated to the testing of potentially counterfeit products around the world. *See* Heidecker Decl. ¶ 13. These test labs control and limit access to a select set of the Cisco Brand Protection team members, which ensures a well-maintained chain of custody and that there can be no tampering with products before, during, or after examination. *Id.* Each test lab is equipped with specialized tools and product data and information that enables the testing engineer to compare suspect products with authentic products. *Id.* ¶ 14.

The largest of Cisco's product authentication test labs is located in San Jose, California. *Id.*¶ 13. Each suspect transceiver that was purchased from Defendants was initially delivered by the Defendant to an address in Brooklyn, New York. *Id.* ¶ 16; Vogel Decl. ¶¶ 8, 19, 24, 27, 31-32. Then, under a stringent chain of custody, each suspect product was shipped to Cisco's San Jose test lab. *See id.* ¶¶ 12-13, 20-21, 28-29, 34-35; Heidecker Decl. ¶ 16.

At the San Jose test lab, Michael Heidecker, a Cisco expert in product testing, analysis, and authentication, reviewed supposedly Cisco transceivers received from the Defendants to determine whether they were counterfeit. *See generally* Heidecker Decl. As set forth in more detail below, Mr. Heidecker first personally evaluated each product using Cisco's standard techniques for evaluating potential counterfeits, and in each case determined from his review that

the Defendants' product was in fact counterfeit. *Id.* ¶ 16. If an OEM was identified on the counterfeit product label, Mr. Heidecker provided images of the suspect product to the OEM. *Id.* Each OEM identified a set of potentially counterfeit attributes, which were evaluated by the OEM's test engineer, and in each case, the OEM's assigned test engineer also determined that the suspect transceiver was counterfeit. *Id.* Each OEM provided its findings to Mr. Heidecker. *Id.* Mr. Heidecker subsequently reviewed each OEM's findings, confirmed them, and incorporated them into a final comprehensive analysis of each counterfeit transceiver. *Id.*

These analyses are set forth in greater detail in Mr. Heidecker's declaration which is submitted herewith.[1] That testing and analysis leaves no room for doubt that every supposed Cisco transceiver purchased from every Defendant is counterfeit. *Id.* ¶ 39. The findings for each Defendant are summarized below.

1. Shenzhen Tianheng

On July 19, 2019, a private investigator purchased six transceivers from Shenzhen Tianheng at the following web address: https://thnetwork.en.alibaba.com/. *See* Vogel Decl. ¶ 6; Heidecker Decl. ¶ 17. Shenzhen Tianheng advertised and sold these transceivers as Cisco-brand transceivers. *See* Vogel Decl. ¶ 5; Heidecker Decl. ¶ 17. As with all the test purchases, Shenzhen Tianheng sent these transceivers to Cisco's investigator in Brooklyn, New York, who then sent the transceivers to Cisco's test lab in San Jose, California, for examination. *See* Vogel Decl. ¶¶ 5-13; Heidecker Decl. ¶ 17.

[1] Because the written analyses describe in detail the differences between the counterfeits and authentic product and how Cisco makes those determinations, they would offer a roadmap to counterfeiters like Defendants as to how to improve their counterfeits and/or evade detection. For that reason, Cisco has not attached them to these filings, but will submit them for the Court's *in camera* review upon request.

On August 26, 2019, Mr. Heidecker examined all six suspect transceivers received from Shenzhen Tianheng. See Heidecker Decl. ¶ 19. Each suspect transceiver had a top label that bore the Cisco logo:  . *Id.* Furthermore, the internal memory of each transceiver, known as EEPROM, identified "CISCO" as the vendor. *Id.* The top label of each transceiver had a serial number that purported to identify a particular OEM for the transceiver. Heidecker Decl. ¶ 20. After his own analysis and testing, Mr. Heidecker provided images of the transceivers to the OEMs identified on the product labels, and those OEMs' product engineers reviewed and analyzed the images and provided their findings. *Id.* For all six suspect transceivers, both Mr. Heidecker and the respective OEMs confirmed that the products are clearly counterfeit in light of the many differences between them and authentic Cisco transceivers. *Id.* These differences include, but are not limited to:

- For genuine Cisco transceivers, the product label serial number and security label serial number are unique numbers that match up. The product label serial number and security label serial number on the Shenzhen Tianheng transceivers do not match.
- Genuine Cisco transceivers are manufactured according to specific design and build standards, and use approved, genuine components. The counterfeit transceivers do not match Cisco's OEM build and design standards and use unapproved, non-genuine components.
- The EEPROM—the internal memory—of genuine Cisco transceivers identifies various product attributes, including the product part number, the vendor, the product serial label number, and a date code. The product attributes contained within the EEPROM for each counterfeit transceiver are incorrect and do not accurately reflect the attributes of a genuine Cisco transceiver.

Heidecker Decl. ¶ 21.

2. Dariocom

Dariocom is an Amazon seller, and through Amazon.com, sold two transceivers, advertised and sold as Cisco-brand receivers, to Cisco's private investigator on July 23, 2019. *See* Vogel Decl. ¶ 30; Heidecker Decl. ¶ 22. As with the transceivers received from Shenzhen

Tianheng, each of the two Dariocom transceivers had a top label that bore the Cisco logo ( ), and the EEPROM for each transceiver identified "CISCO" as the vendor. Heidecker Decl. ¶ 24. Each transceiver also had a product label serial number supposedly identifying the OEM for the transceiver. *Id.* ¶ 25. For both suspect transceivers received from Dariocom, both Mr. Heidecker and the respective OEMs confirmed that the products were clearly counterfeit in light of the many differences between them and authentic Cisco transceivers. *Id.* ¶¶ 25-26. These differences include, but are not limited to, the differences set forth above in connection with counterfeit receivers received from Shenzhen Tianheng: (1) the non-matching product label and security label serial numbers; (2) the use of non-genuine components that fail the OEM build and design standards; and (3) the incorrect and inaccurate product attributes contained in the EEPROM of each transceiver. *Id.*

3. Gezhi Photonics

On August 23, 2019, a private investigator purchased two transceivers, advertised and sold as Cisco-brand transceivers, from Gezhi Photonics at the following web address: https://gezhiphotonics.en.alibaba.com/. *See* Vogel Decl. ¶¶ 14-16; Heidecker Decl. ¶ 27.

The EEPROM for each Gezhi Photonics transceiver identified "CISCO" as the vendor. *See* Heidecker Decl. ¶ 29. The top label of the suspect transceivers sold by Gezhi Photonics did not indicate an OEM, and so Cisco was unable to provide the transceivers to an OEM for additional analysis. *Id.* ¶ 30. Because authentic product always contains a top label that indicates an OEM, the lack of such information on the top label of the transceivers sold by Gezhi Photonics is itself evidence that the product is counterfeit. *Id.* Mr. Heidecker's testing and analysis confirmed that both of the transceivers received from Gezhi Photonics were clearly

counterfeit in light of the many differences between them and authentic Cisco transceivers. *Id.* ¶ 31. These differences include, but are not limited to:

- The top label of each Gezhi Photonics transceiver is not consistent with authentic Cisco transceiver top labels. The product label serial number on each Gezhi Photonics transceiver does not meet the Cisco-approved product label serial number format or nomenclature.
- The attributes contained within the EEPROM for each Gezhi Photonics transceiver are incorrect and do not accurately reflect the attributes of a genuine Cisco transceiver.
- As noted above, the Gezhi Photonics transceivers do not identify the OEM, which always appears on authentic Cisco transceivers.

Id.

4. Shenzhen Sourcelight

On September 11, 2019, a private investigator purchased two transceivers, advertised and sold as Cisco-brand transceivers, from Shenzhen Sourcelight at the following web address: https://sourcelighten.en.alibaba.com/. *See* Vogel Decl. ¶¶ 22-25; Heidecker Decl. ¶¶ 33.

The EEPROM for each Shenzhen Sourcelight transceiver identified "CISCO" as the vendor. *See* Heidecker Decl. ¶ 35. As with the counterfeit transceivers received from Gezhi Photonics, the top label of the suspect transceivers sold by Shenzhen Sourcelight did not indicate an OEM, which itself is evidence that the product is counterfeit. *Id.* ¶ 36. Mr. Heidecker's testing and analysis confirmed that both of the transceivers received from Shenzen Sourcelight were clearly counterfeit in light of the many differences between them and authentic Cisco transceivers. *Id.* ¶ 37. These differences include, but are not limited to, the differences set forth above in connection with counterfeit receivers received from Gezhi Photonics: (1) the incorrect top label that does not match Cisco's authorized format or nomenclature; (2) the incorrect and inaccurate product attributes contained in the EEPROM of each transceiver; and (3) the failure to identify an OEM. *Id.*

ARGUMENT

I. CISCO IS ENTITLED TO IMMEDIATE INJUNCTIVE RELIEF

Cisco seeks a temporary restraining order to immediately stop Defendants' trafficking of counterfeit Cisco transceivers and ensure that evidence, including the counterfeit products themselves, is preserved. The issuance of such injunctions is commonplace in actions under the Lanham Act. *See, e.g.*, *McDonald's Corp. v. Robertson*, 147 F.3d 1301, 1310 (11th Cir. 1998) ("[T]rademark actions are common venues for the issuance of preliminary injunctions") (internal quotation marks and citations omitted); *Multi-Local Media Corp. v. 800 Yellow Book, Inc.*, 813 F. Supp. 199, 202 (E.D.N.Y. 1993) ("Federal courts have long recognized the need for immediate injunctive relief in trademark infringement cases due to the amorphous nature of the damage to the trademark and the resulting difficulty in proving monetary damages."). Here, where Defendants have been caught red-handed selling dangerous counterfeit transceivers into the United States, the need for immediate injunctive relief is especially apparent.

A plaintiff's burden for obtaining preliminary injunctive relief is to demonstrate "that it is likely to succeed on the merits, that [it] is likely to suffer irreparable harm in the absence of preliminary relief, that the balance of equities tips in [its] favor, and that an injunction is in the public interest." *Winter v. Natural Res. Def. Council, Inc.* 555 U.S. 7, 20 (2008). Cisco easily meets all of those elements here.

A. Cisco Has a Strong Likelihood of Success on the Merits

Among other claims, Cisco has alleged causes of action under the Lanham Act, as well as state law, for violating Cisco's trademark rights by selling counterfeit product. Cisco can prevail on its trademark claims by showing "(1) that it owns a valid, protectable trademark; (2) that the defendants used the registrant's trademark in commerce and without consent; and (3) that there was a likelihood of consumer confusion." *Proctor & Gamble Co. v. Quality King Distribs., Inc.*

123 F. Supp. 2d 108, 113 (E.D.N.Y. 2000); *see also Tanning Research Labs., Inc. v. Worldwide Import & Exp. Corp.*, 803 F. Supp. 606, 608-09 (E.D.N.Y. 1992).

None of these elements is remotely in question here. As described above, Cisco owns valid trademarks for the products at issue. Williams Decl. ¶¶ 4-9 & Ex. 1. Defendants are "using" those marks in interstate commerce by selling counterfeit Cisco product into the United States, including into this District.[2] The caselaw overwhelmingly confirms that because Defendants have sold counterfeit transceivers intended to look exactly like genuine Cisco transceivers, likelihood of consumer confusion is established as a matter of law. *See El Greco Leather Prods. Co. v. Shoe World, Inc.*, 806 F.2d 392, 396 (2d Cir. 1986) ("it is plain" that the sale of products that are "not genuine" violates the Lanham Act); *RJR Foods, Inc. v. White Rock Corp.*, 603 F.2d 1058, 1060 (2d Cir. 1979) ("defendant's conscious imitation ... supports at least a presumption that the similarity will cause customer confusion"); *Omega Importing Corp. v. Petri-Kine Camera Co.*, 451 F.2d 1190, 1194 (2d Cir. 1971) (Friendly, C.J.) ("The probabilities of confusion from the sale of another [product] bearing the identical name are too obvious to require detailed proof"); *Koon Chun Hing Kee Soy & Sauce Factory, Ltd. v. Star Mark Mgmt., Inc.*, 2007 U.S. Dist. LEXIS 1404, at *32-*33 (E.D.N.Y. Jan. 8, 2007), *aff'd*, 409 Fed. App'x. 389 (2d Cir. 2010); *Lorillard Tobacco Co. v. Jamelis Grocery, Inc.*, 378 F. Supp. 2d 448, 455 (S.D.N.Y. 2005); *Philip Morris USA Inc. v. Felizardo*, 2004 U.S. Dist. LEXIS 11154, at *18 (S.D.N.Y. June 18, 2004) ("[C]ounterfeit marks are inherently confusing."); *Gucci Am., Inc. v. Duty Free Apparel, Ltd.*, 286 F. Supp. 2d 284, 287 (S.D.N.Y. 2003) ("[C]ounterfeits, by their

[2] Defendants Shenzhen Tianheng, Gezhi Photonics, Shenzhen Sourcelight, and Dariocom are the corporate entities that sold the counterfeit product. The individuals named as Defendants are personally liable for the counterfeiting because as corporate officers each was a moving, active, conscious force behind their respective corporations' infringement. *Bambu Sales Inc. v. Sultana Crackers Inc.,* 683 F. Supp. 899, 913 (E.D.N.Y. 1988); *Procter & Gamble Co. v. Xetal, Inc.,* 2006 U.S. Dist. LEXIS 24342, at *6 (E.D.N.Y. Mar. 23, 2006).

very nature, cause confusion."); *Procter & Gamble Co.*, 123 F. Supp. 2d at 115 ("It would be difficult to imagine a clearer case of consumer confusion than the instant case in which defendants, acting in direct competition with the plaintiff, sold counterfeit products on which plaintiff's registered marks appear in their entirety.'" (citation omitted)).[3]

Notably, trademark infringement, including counterfeiting, is a strict liability offense. *Sunward Elecs., Inc. v. McDonald*, 362 F.3d 17, 25 (2d Cir. 2004) ("[I]t is well established that wrongful intent is not a prerequisite to an action for trademark infringement . . . and that good faith is no defense." (citations and internal quotations omitted)); *Hard Rock Café Licensing Corp. v. Concession Servs., Inc.*, 955 F.2d 1143, 1152 n.6 (7th Cir. 1992) ("Sellers bear strict liability for violations of the Lanham Act."); *Taubman Co. v. Webfeats*, 319 F.3d 770, 775 (6th Cir. 2003); *Philip Morris USA Inc. v. Shalabi*, 352 F. Supp. 2d 1067, 1073-74 (C.D. Cal. 2004). Therefore, Defendants are liable under the Lanham Act regardless of whether they were aware of the counterfeit nature of the products they sold. *Id.*; *see also Philip Morris USA Inc. v. Liu*, 489 F. Supp. 2d 1119, 1122 (C.D. Cal. 2007). Here, there can be no doubt they were aware.

Cisco of course did not, and cannot, supervise the quality or safety of the counterfeit products sold by the Defendants. Consumers are therefore likely to be not only confused, but also deterred from being Cisco customers after they receive these inferior and potentially dangerous counterfeit products that Defendants falsely present as authentic Cisco transceivers. *El Greco*, 806 F.2d at 395 ("One of the most valuable and important protections afforded by the Lanham Act is the right to control the quality of the goods manufactured and sold under the

[3] Because counterfeit marks are inherently confusing, there is no need to analyze the so-called *Polaroid* factors to determine the likelihood of confusion between the genuine and the counterfeit goods. *Jamelis Grocery*, 378 F. Supp. 2d at 455 (citing *Polaroid Corp. v. Polarad Elecs. Corp.*, 287 F.2d 492, 495-96 (2d Cir. 1961)). Counterfeits create consumer confusion as a matter of law. *Id.*

holder's trademark."); *see also Warner-Lambert Co. v. Northside Dev. Corp.*, 86 F.3d 3, 6 (2d Cir. 1996) ("Distribution of a product that does not meet the trademark holder's quality control standards may result in the devaluation of the mark by tarnishing its image.").

In short, Cisco has presented detailed and unimpeachable evidence that all of the transceivers purchased from the Defendants are counterfeit, and it is black-letter law that the Defendants are strictly liable for their sale of counterfeit products. Cisco's claims under the Lanham Act claims are not merely likely to succeed: they are virtually certain to succeed.

B. Cisco Is Suffering Irreparable Harm as a Result of Defendants' Activities

Where, as here, a Lanham Act plaintiff has succeeded in showing a likelihood of confusion, irreparable injury "almost inevitably follows." *Omega Importing Corp.*, 451 F.2d at 1195. The reason is simple: "because the losses of reputation and goodwill and subsequent loss of customers that Plaintiff will suffer are not precisely quantifiable[,] remedies at law cannot adequately compensate Plaintiff for its injuries." *Pretty Girl, Inc. v. Pretty Girl Fashions, Inc.*, 778 F. Supp. 2d 261, 270 (E.D.N.Y. 2011); *see also Church of Scientology Int'l v. Elmira Mission*, 794 F.2d 38, 44 (2d Cir. 1986) ("[A]llowing defendants the opportunity to reduce the marks' reputational value and goodwill by its continued unauthorized use constitutes the irreparable harm that is requisite to the issuance of the preliminary injunction."); *New York City Triathlon, LLC v. NYC Triathlon Club*, 704 F. Supp. 2d 305, 325 (S.D.N.Y 2010) ("It is well-settled that a trademark owner's loss of goodwill and ability to control its reputation constitutes irreparable harm sufficient to satisfy the preliminary injunction standard."); 5 J. Thomas McCarthy, McCarthy on Trademarks § 30:46 (4th ed. 2012) ("[O]nce the trademark owner shows a probability of proving a likelihood of confusion . . . is shown, the trademark owner's business reputation and goodwill are at risk.... Like trying to un-ring a bell, trying to [use

dollars] to 'compensate' after the fact for damage to business goodwill and reputation cannot constitute fair or full compensation.").

There can be no question that in this case the sale of counterfeit Cisco transceivers is causing great harm to Cisco's valuable goodwill and that its continued sale would create a substantial likelihood of irreparable harm to Cisco. Not only is Cisco unable to control any aspect of the counterfeit product being falsely sold under its trademarks, but the counterfeit product is in fact inferior to genuine Cisco transceivers and poses a serious risk to the American public. Immediate injunctive relief is necessary to prevent further irreparable damage to Cisco's reputation and goodwill. *See* Williams Decl. ¶¶ 15-23.

C. The Balance of Equities Tips Decisively in Cisco's Favor

Equitable factors emphatically support the issuance of a temporary restraining order. There is no weight at all on Defendants' side of the equitable scales: Defendants have no right to sell counterfeit Cisco transceivers and thus cannot claim any cognizable hardship from the proposed injunctive relief. On Cisco's side of the scales, every sale of a counterfeit Cisco transceiver diminishes the value of Cisco's trademarks and causes harm to Cisco's reputation. *See, e.g.*, *Microsoft Corp. v. ATEK 3000 Computer Inc.*, 2008 U.S. Dist. LEXIS 56689, at *17 (E.D.N.Y. Jul. 23, 2008). More than that, the counterfeit transceivers are defective and dangerous, and pose a threat to public safety and security, which on its own justifies immediate injunctive relief. *See, e.g.*, *McDonald's Corp. v. Robertson*, 147 F.3d 1301, 1310 (11th Cir. 1998); *Burger King Corp. v. Stephens*, 1989 U.S. Dist. LEXIS 14527 at *33 (E.D. Pa. Dec. 6, 1989).

D. An Injunction Is in the Public Interest

Finally, an injunction is in the public interest because it will protect the public from unlawful and defective counterfeit products. "When a trademark is said to have been infringed,

what is actually infringed is the right of the public to be free of confusion and the synonymous right of the trademark owner to control his products' reputation." *Cytosport, Inc. v. Vital Pharms., Inc.*, 617 F. Supp. 2d 1051, 1081 (E.D. Cal. 2009) (internal citation omitted). The public interest is especially clear here, where the use of authentic Cisco transceivers is essential to the ability of innumerable American persons, businesses, and organizations to connect to the internet and to securely send and store information—including governmental offices, U.S. military organizations, and hospitals. *See, e.g.*, *Tartell v. S. Fla. Sinus & Allergy Ctr., Inc.*, 2013 U.S. Dist. LEXIS 191404, at *33 (S.D. Fla. Jan. 25, 2013) (finding "that it is in the public interest to enforce the trademark laws against ... appropriation of others' marks ... especially when that conduct causes a likelihood of confusion among those selecting medical doctors.").

E. At an Absolute Minimum, There Are Serious Questions Going to the Merits and the Balance of Hardships Decidedly Favors Plaintiffs

Even if there were any doubt—and Cisco respectfully submits there is not—that Cisco is likely to prevail on the merits if its claims, a temporary restraining order would still be appropriate because there are at absolute minimum "sufficiently serious questions going to the merits to make them a fair ground for litigation plus a balance of hardships tipping decidedly toward the party requesting the preliminary relief." *Sunward Elecs., Inc. v. McDonald*, 362 F.3d 17, 24 (2d Cir. 2004). Cisco has submitted clear evidence that Defendants sold counterfeit Cisco transceivers featuring counterfeits of Cisco's valid, protectable trademarks. Since trademark infringement is a strict liability offense, Cisco's evidence easily meets and exceededs the "serious questions going to the merits" standard, and the balance of hardships in this case is overwhelmingly in Cisco's favor.

II. CISCO IS ENTITLED TO AN *EX PARTE* ORDER FREEZING DEFENDANTS' ASSETS, DISABLING AND TRANSFERRING TO CISCO DEFENDANTS' SELLER IDENTIFICATIONS AND DOMAIN NAMES, AND PROHIBITING ACCESS TO AND FULFILLMENT OF PRODUCTS BEARING INFRINGING CISCO MARKS

Where, as here, a plaintiff seeks equitable remedies, including lost profits, under the Lanham Act, 15 U.S.C. §§ 1116(a) and 1117, a federal court has the "inherent equitable powers to order preliminary relief, including an asset freeze, in order to assure the availability of permanent relief." *Levi Strauss & Co. v. Sunrise Int'l Trading, Inc.*, 51 F.3d 982, 987 (11th Cir. 1995). Cisco seeks the entry of an *ex parte* order providing various types of injunctive relief. As set forth in detail below, the relief that Cisco seeks is routinely granted in cases involving the online sale of counterfeit goods.

The requested injunctive relief will preserve the status quo while immediately halting the Defendants' ability to advertise the counterfeits and sell them into the United States. Moreover, the requested injunctive relief will help secure the participation of the Defendants, all of whom are based in China, in this litigation. There is no question that this Court has personal jurisdiction over foreign counterfeiters who sell into this District; however, overseas counterfeiters often ignore the filing of a U.S. lawsuit against them, especially when they reside in countries where it is difficult or impossible to enforce the judgment of a U.S. court. Absent injunctive relief, overseas counterfeiters can also easily move their assets and operations to a different corporate form or simply sell the counterfeits under a different user or store name. As explained in further detail below, the requested relief will ensure that the Defendants receive prompt and actual notice of this action, and will provide significant incentive for them to retain counsel, appear before this Court, and participate in this litigation.

A. The Court Should Issue an *Ex Parte* Order Freezing Defendants' Assets

First, Cisco seeks an order freezing Defendants' assets. Courts recognize that counterfeiters make their living by secrets and subterfuge, and therefore are likely to "hide their allegedly ill-gotten funds" if their assets are not frozen. *Reebok Int'l, Ltd. v. Marnatech Enters., Inc.*, 970 F.2d 552, 563 (9th Cir. 1992); *accord Chanel, Inc. v. Classic-Bag-Shop*, 2019 U.S. Dist. LEXIS 42688, at *10 (S.D. Fla. Mar. 14, 2019) ("In light of the inherently deceptive nature of the counterfeiting business ... Plaintiff has good reason to believe Defendants will hide or transfer their ill-gotten assets beyond the jurisdiction of this Court unless those assets are restrained."). Those concerns apply with special force in cases like the instant action, where overseas counterfeiters make use of online platforms to sell and distribute illegal counterfeits into the United States. Moreover, the freezing of Defendants' assets will certainly capture their attention, and will incentivize them to appear before the Court.

In its Complaint, Cisco seeks under the Lanham Act an accounting and disgorgement of Defendants' illicit profits from their sale and distribution of counterfeit Cisco products that fraudulently bear Cisco's trademarks. "Because the Lanham Act authorizes the district court to grant [plaintiff] an accounting of [defendant's] profits as a form of final equitable relief, the district court had the inherent power to freeze [defendant's] assets in order to ensure the availability of that final relief." *Reebok*, 970 F.2d at 559; *see also Motorola Inc. v. Abeckaser*, 2009 U.S. Dist. LEXIS 40660, at *8 (E.D.N.Y. May 14, 2009); *N. Face Apparel Corp. v. TC Fashions, Inc.*, 2006 U.S. Dist. LEXIS 14226, at *10 (S.D.N.Y. Mar. 30, 2006) (In counterfeiting cases, "[d]istrict courts have the 'authority to freeze those assets which could [be] used to satisfy an equitable award of profits.'"). The purpose of such an order is "to preserve the possibility of an effective accounting of [the counterfeiter's] profits and the return of the profits fraudulently obtained." *Reebok*, 970 F.2d at 560. Moreover, asset freeze orders are

exceptionally effective at capturing the attention of overseas counterfeiters who might otherwise ignore legal processes in the United States. Accordingly, in order to ensure that the accounting and lost profits sought by Cisco are available at the conclusion of this action, and to secure the participation of Defendants in this action, Cisco respectfully submits that the Court should issue an *ex parte* order freezing the Defendants' assets.

Notably, the Court's authority to freeze assets is not limited to assets within this District, nor even to assets within the United States. *See, e.g., Citronelle-Mobile Gathering, Inc. v. Watkins*, 943 F.2d 1297, 1301 (11th Cir. 1991) (upholding district court order directing "banks or financial institutions wherever located to freeze the judgment debtors' assets." (internal quotation marks omitted)). Similarly, this Court is armed with further authority under the All Writs Act, 28 U.S.C. § 1651, to issue such orders requiring the cooperation of banks and other non-parties that may have physical custody of defendants' assets or have provided payment services to any of the Defendants. *See Burr & Forman v. Blair*, 470 F.3d 1019, 1026-27 (11th Cir. 2006) ("The power to issue writs under the Act is not circumscribed by the identity of the parties immediately before the court; at the court's discretion, writs may be issued to third parties who are in a position to frustrate a court's administration of its jurisdiction." (citing *United States v. New York Tel. Co.*, 434 U.S. 159, 174 (1977)). Accordingly, Cisco respectfully submits that the asset freeze order should freeze all assets of Defendants, wherever and in whomever's possession they may be found, and issue such subsequent and additional injunctive orders against non-parties to this action as may be necessary to enable Cisco to fully enforce this asset freeze order.

Cisco further respectfully submits that the order should be issued *ex parte* to ensure that Cisco's right to an equitable accounting of Defendants' profits is not impaired. *See Columbia Pictures Indus., Inc. v. Jasso*, 927 F. Supp. 1075, 1077 (N.D. Ill. 19996) (observing that

"proceedings against those who deliberately traffic in infringing merchandise are often rendered useless if notice is given to the infringers"). The Defendants here are Chinese companies and their principals who most likely hold most of their assets in China, and so Defendants are uniquely well-positioned to easily hide or dispose of their assets if given prior notice, which would render an accounting by Cisco meaningless.

B. The Court Should Issue an Order Disabling, and Transferring to Cisco, All of Defendants' Seller Identifications and Domain Names

Defendants are knowingly and intentionally promoting, advertising, selling, and distributing products bearing counterfeit CISCO Marks within this District and throughout the United States. They are doing so by operating eCommerce stores on third-party marketplaces ("eCommerce Websites") such as Amazon and Alibaba, using their respective seller identifications on those third-party websites. And in addition to their use of third-party eCommerce Websites like Amazon and Alibaba, the Defendants also conduct their illicit business on separate, fully interactive, commercial internet websites ("Domain Names"). A list of known seller identifications, eCommerce Websites, and Domain Names that Defendants use to advertise, offer for sale, and sell counterfeit Cisco products is submitted as Schedule A to the White Declaration.

To preserve the status quo while also preventing Defendants from displaying website content concerning the counterfeits at issue, Cisco seeks an order freezing Defendants' seller identifications and Domain Names. Cisco also requests that the order transfer to Cisco, pending final hearing and determination of this action, all known and later-discovered seller identifications and Domain Names used by Defendants to advertise, offer for sale, or sell Cisco-marked products. Finally, Cisco requests that the order disable and redirect the offending Domain Names as a means of affording Cisco interim relief that avoids the irreparable harm

caused by the advertisement and sale of these counterfeits. Once they become aware of litigation against them, defendants that sell counterfeit goods via eCommerce websites and domain names easily can, and often will, take simple steps to conceal and/or move their illicit business to other channels, including modifying the domain registration; changing payment accounts; redirecting consumer traffic to other seller identifications, private messaging accounts, and domain names; and transferring assets and ownership of seller identifications and Domain Names. Such actions would thwart the Court's ability to grant meaningful relief. *See, e.g.*, *Chanel, Inc. v. The Individuals, Partnerships, and Unincorporated Ass'ns Identified on Schedule "A"*, Case No. 19-cv-60491-UU, Dkt. No. 8 at 7 (S.D. Fla. Feb. 28, 2019). Here, an order prohibiting Defendants from transferring their seller identifications and Domain Names poses no burden on Defendants and ensures that the Court, after fully hearing the merits of this action, will be able to afford Cisco full relief. Courts have granted this precise relief in actions where the defendants' instrumentalities of infringement have been e-commerce stores, domain names, and associated websites and accounts. *See, e.g.*, *id.*; *Gucci Am., Inc. v. a.m.m.mall*, Case No. 18-cv-62229-UU (S.D. Fla. Sept. 21, 2018) (order restraining the transfer of e-commerce stores operating via marketplace platforms); *Tiffany (NJ) LLC v. dorapang franchise store*, Case No. 18-cv-61590-UU (S.D. Fla. July 16, 2018) (same); *Chanel, Inc. v. brand234.com*, Case No. 18-cv-60615-JEM (S.D. Fla. Mar. 27, 2018) (same); *cf. McGraw-Hill Global Educ. Holdings, LLC v. Khan*, 323 F. Supp. 3d 488, 493 (S.D.N.Y. 2018) (discussing court's preliminary injunction order enjoining defendants from transferring ownership or control of the websites and domain names associated with defendants' copyright infringement).

The Lanham Act expressly contemplates this relief. Entities known as domain name registrars exercise effective control over whether domain names can be transferred, and so the

Lanham Act explicitly provides for registrars to deposit domain name certificates with the Court, allowing the Court to exercise control over the domain names. *See* 15 U.S.C. § 1114(2)(D); 15 U.S.C. § 1125(d)(2)(C); *see also Philip Morris USA, Inc. v. Otamedia Ltd.*, 331 F. Supp. 2d 228, 230 (S.D.N.Y. 2004) (affirming registrar's decision to deposit certificate with court where registrant used website to make infringing sales); *cf. Las Vegas Sands Corp. v. Fan Yu Ming*, 360 F. Supp. 3d 1072, 1076, 1082 (D. Nev. Jan. 9, 2019) (granting preliminary injunction and ordering domain name registrar and registries to maintain infringing domains on "hold and lock"). This assures the Court and the parties that the ownership of the domain names will not change while the action is proceeding. Cisco therefore respectfully requests that the Court order the registrars for the Domain Names being used and controlled by Defendants to deposit domain certificates with Cisco.

Cisco further seeks the relief of having the Defendants' Domain Names automatically redirect to a website that provides notice of this action. Specifically, Cisco respectfully requests that the Court's order require the registrars and the registries that maintain what are known as the top-level domain zone—e.g., ".com" and ".org"—files for the Defendants' Domain Names change the registrar of record for the Domain Names to a holding account with a registrar of Cisco's choosing, where they will be held during the pendency of this action. *See, e.g.*, *Chanel, Inc. v. chanellook.com*, Case No. 18-cv-62496-UU (S.D. Fla. Oct. 19, 2018) (granting order changing registrars); *Chanel, Inc. v. Aaachanelshop.ru*, 2019 U.S. Dist. LEXIS 175511, at *4-5 (S.D. Fla. Oct. 8, 2019) (same); *Chanel, Inc. v. amazing456.com*, Case No. 18-cv-63046-RNS (S.D. Fla. Jan. 8, 2019) (same). In other words, upon redirection, a copy of all of the pleadings, other documents, and Court orders issued in this matter will be immediately visible to Defendants the moment they type any of their own domain names into their web browsers. *See,*

e.g., *Gucci Am., Inc. v. Gucci-Taschens.com*, 2019 U.S. Dist. LEXIS 170582, at *15-16 (S.D. Fla. Sept. 6, 2019); *Luxottica Grp. S.p.A. v. P'ships & Unincorporated Ass'n Identified on Schedule "A"*, 391 F. Supp. 3d 816, 820 (N.D. Ill. May 24, 2019) (confirming grant of *ex parte* TRO transferring defendants' domain names to plaintiffs' control in order to provide notice of the proceedings by redirecting the domain names to a website hosting the complaint, TRO, and other relevant documents). The Domain Names would remain in the legal ownership of Defendants, but they would no longer be able to display infringing content and counterfeit products. This would not only prevent further infringing conduct, but would serve as the most effective means of notifying each overseas Defendant of the pendency of the action and the relief sought by Cisco. There will be no doubt of the Defendants' knowledge of this action and ability to seek relief from this Court when the pleadings and the Court's contact information are posted on Defendants' own websites.

C. An Order Should Be Issued Cutting Off Access to and Prohibiting Fulfillment of Any of Defendants' Products Bearing CISCO Marks

Finally, Cisco seeks a preliminary order barring access to Defendants' listings of counterfeit Cisco products and prohibiting the fulfillment of orders for those products. This relief is a necessary and appropriate means of immediately stopping Defendants' fraud on the public and on Cisco, and will further incentivize Defendants to participate in this litigation.

Specifically, Cisco respectfully requests that the Court order that any eCommerce Website who is provided with notice of the injunction disable and be restrained from displaying or facilitating access to any listings or advertisements or associated images, or otherwise providing any service or payment to any of the Defendants (and any individuals or entities acting in concert or participation with Defendants) in relation to any Cisco-marked products. This includes all accounts operating under the Defendants' seller identifications, listings, and

associated images identified by the Amazon Standard Identification Numbers ("ASIN"), and any other listings and images of products bearing the CISCO Marks associated with any ASIN linked to the same sellers or linked to any other alias seller identifications being used or controlled by Defendants to offer for sale products bearing CISCO Marks.[4]

Courts have routinely granted this relief. *See, e.g.*, *Apple Corps Ltd. v. 3w store*, Case No. 18-cv-60656-UU (S.D. Fla. Mar. 28, 2018) (granting order requiring internet marketplace website operators to cease facilitating access to all listings and associated images of the products bearing counterfeits or infringements of the plaintiff's trademarks); *Chanel, Inc. v. bethbass*, Case No. 16-cv-61674-UU (S.D. Fla. July 18, 2016) (same); *Chanel, Inc. v. replicachanelbag*, Case No. 18-cv-62860-BB (S.D. Fla. Nov. 27, 2018) (granting order requiring social media website operators to cease facilitating access to all listings and associated images of the products bearing counterfeits or infringements of the plaintiff's trademarks).

To ensure that any pending or ongoing sales of counterfeit Cisco transceivers are not completed, Cisco respectfully requests that the Court's order include that, upon Cisco's request, Defendants and any eCommere Website operator or administrator who is provided with notice of the temporary restraining order—including but not limited to Amazon.com and Alibaba.com—cease fulfillment of Defendants' Cisco-branded products. In conjunction, Cisco seeks an order requiring any internet search engine, such as Google, Bing, and Yahoo, ("Internet Search Engines") remove from its index and search results any URL, domain name, or other content

[4] The ASIN is a unique 10-digit alphanumeric identifier Amazon assigns to each product. Sellers can create a variational relationship between products in regards to name and size. When doing so, the ASIN identified in the Product Information/Description segments represents the core product and a different ASIN may be assigned based on variations thereof, as identified in the URLs. The ASINs for the Cisco-branded transceivers were obtained from the Product Information/Description segments, the URLs of the infringing Cisco-branded transceivers, or active links embedded in the webpage captures of the Cisco-branded transceivers.

owned, controlled, or otherwise associated with any Defendant's advertisement, offer for sale, or sale of Cisco-marked products. Cisco further requests that any non-party that provides transportation services in relation to the Cisco-marked products that Defendants sell ("Common Carriers") be restrained from fulfilling any pending or accepting any future shipments by any of the Defendants. Finally, Cisco requests that any eCommerce Websites or Common Carriers sequester any of Defendants' Cisco-branded products in their inventory, possession, custody, or control, and turn over to Cisco (or a person or entity designated by Cisco) for inspection and then to be held by Cisco until further order of this Court.

Such relief is necessary to prevent the public from continuing to be defrauded by Defendants' illegal activities and avoids continuing irreparable harm to Cisco. *See, e.g.*, *Chanel, Inc. v. Amasek*, Case No. 18-cv-62304-BB (S.D. Fla. Sept. 28, 2018) (granting order requiring internet marketplace website operators to immediately cease fulfillment of and sequester all goods bearing one or more of the plaintiff's trademarks, and hold such goods in trust for the Court during the pendency of the action); *Goyard St-Honore v. abraham ben*, Case No. 18-cv-61771-WPD (S.D. Fla. Aug. 2, 2018) (same). The evidence submitted herewith conclusively demonstrates that Defendants are selling counterfeit Cisco products. Whatever interests the Defendants might have are heavily outweighed by Cisco's equitable and legal interest in removing counterfeit products from the marketplace, as well as by the public interest in having dangerous counterfeits removed from American commerce.

III. CISCO IS ENTITLED TO EXPEDITED DISCOVERY

Cisco seeks expedited discovery so that it may investigate, trace, and pursue the manufacture and distribution of counterfeit Cisco transceivers in an effort to permanently banish them from the market. Federal courts have broad discretion to expedite the normal pace of discovery in cases seeking temporary or preliminary injunctive relief. 28 U.S.C. § 1657 directs

that "the court shall expedite the consideration of ... any action for temporary or preliminary injunctive relief." Similarly, Rule 26(d) allows for expedited discovery, and an Advisory Committee comment to that Rule notes that expedited discovery "will be appropriate in some cases, such as those involving requests for a preliminary injunction." Advisory Comm. Note to Fed. R. Civ. P. 26(d). Moreover, Rule 30(a)(2)(A)(iii) provides that the Court may grant leave to take depositions "before the time specified" in the discovery rules, and Rule 34(b)(2)(A) provides that "[a] shorter or longer time may be ... ordered by the court" for the production of documents than the rules would otherwise allow. Finally, Congress recognized that there is a special need for expedited discovery in counterfeiting cases, specifying in the Trademark Counterfeiting Act that a court may modify the time limits for discovery "to prevent the frustration of the purposes of [a seizure order] hearing." 15 U.S.C. § 1116(d)(10)(B).

Like injunctive relief, "[c]ourts have recognized that accelerated discovery may be particularly appropriate in cases of trademark counterfeiting." *Dell Inc. v. BelgiumDomains, LLC*, 2007 U.S. Dist. LEXIS 98676, at *18 (S.D. Fla. Nov. 20, 2007); *see also N. Atl. Operating Co. v. Evergreen Distribs., LLC*, 293 F.R.D. 363, 367 (E.D.N.Y. 2013) ("In counterfeiting cases, expedited discovery may need to be granted because discovery on an expedited basis may very well lead to evidence of continuing infringement by this defendant or others; it may also lead to the discovery of future plans to infringe or the discovery of additional infringing merchandise.") (internal quotation marks and citation omitted). "In situations where time is of the essence, courts have found good cause to grant expedited discovery." *Malibu Media, LLC v. Doe*, 2014 U.S. Dist. LEXIS 192209, at *3 (M.D. Fla. Nov. 4, 2014) (internal quotation marks and citation omitted). There are numerous examples from within this Circuit and elsewhere of courts granting expedited discovery in trademark cases involving conduct far less extreme than the sale

of networking devices critical to America's informational infrastructure. *See, e.g.*, *Chanel, Inc. v. Classic-Bag-Shop*, No. 0:19-cv-60491-UU, Dkt. No. 33 (S.D. Fla. Mar. 14, 2019); *Chanel, Inc. v. brand234.com*, No. 0:18-cv-60615-JEM, Dkt. No. 10 (S.D. Fla. Mar. 27, 2018); *Innovation Ventures, LLC v. Ultimate One Distrib. Corp.*, No. 1:12-cv-05354-KAM-RLM, Dkt. No. 290 (E.D.N.Y. Dec. 28, 2012).

Here, as set forth in the accompanying proposed order, Cisco seeks three types of expedited discovery:

First, in order to identify any sources from whom Defendants are purchasing counterfeit Cisco transceivers and any other distributors to whom Defendants are supplying counterfeit Cisco transceivers, Cisco seeks production from each Defendant of documents sufficient to show the names, addresses, and contact information of all individuals and entities each Defendant purchased Cisco transceivers from and sold Cisco transceivers to, along with the quantities and prices of all such purchases and sales. *See, e.g.*, *Dentsply Sirona Inc. v. L I K Supply, Corp.*, 2016 U.S. Dist. LEXIS 91894, at *24-25 (N.D.N.Y. July 15, 2016) (granting motion for expedited discovery of the identities of the sources and purchasers of the counterfeit products, and any participants in the unlawful conduct).

Second, Cisco also seeks expedited production from any non-party who is affiliated with or providing services to Defendants, including but not limited to any eCommerce Website, Internet Search Engine, Common Carrier, or financial institution or payment service, of documents concerning (a) the names, addresses, and other contact information of each Defendant and all entities and individuals associated, in concert, or in participation with that Defendant; (b) each Defendant's operations, methods of payment, transportation, and listing history concerning their advertisement and sale of Cisco-marked products; (c) each Defendant's online marketplace

accounts; and (d) any financial accounts owned or controlled by the Defendants and any entities and individuals associated, in concert, or in participation with them. Discovery of these accounts and services is necessary to ensure that Defendants' unlawful activities will be contained. *See, e.g.*, *McGraw-Hill Global Educ. Holdings, LLC*, 323 F. Supp. 3d at 493 (discussing court's preliminary injunction order directing defendants to locate all accounts connected to defendants' websites and refrain from transferring or withdrawing any funds from therein); *Deckers Outdoor Corp. v. The Partnerships*, Case No. 15-cv-3249 (N.D. Ill. Apr. 21, 2015).

Third, to the extent the privacy protection service for any of Defendants' seller identifications or Domain Names has concealed the registrant's identity and contact information, Cisco seeks disclosure of the true identities and contact information of those registrants.

Cisco has shown good cause for such discovery. *See Cecere v. Cty. of Nassau*, 258 F. Supp. 2d 184, 186 (E.D.N.Y. 2003) (considering the following factors for expedited discovery: "(1) irreparable injury, (2) some probability of success on the merits, (3) some connection between the expedited discovery and the avoidance of the irreparable injury, and (4) some evidence that the injury that will result without expedited discovery looms greater than the injury that the defendant will suffer if the expedited relief is granted") (internal quotation marks and citation omitted). As set forth above, Cisco is suffering irreparable injury and is likely to succeed on the merits. Moreover, the scope of the requested discovery is narrow. *See Federal Express Corp. v. Federal Espresso, Inc.*, 1997 U.S. Dist. LEXIS 19144, at *5 (N.D.N.Y. Nov. 24, 1997) ("the scope of permissible expedited discovery is limited to requests that are more narrowly 'tailored to the time constraints under which both parties must proceed [and] to the specific issues that will have to be determined at the preliminary injunction hearing.'") (citation omitted). Cisco seeks expedited discovery because, as outlined above, it is attempting to locate

the manufacture and distribution of a defective and dangerous counterfeit product and eradicate such products from the market. Finally, the harm to Cisco if discovery proceeds at the ordinary pace will far outweigh any conceivable burden to Defendants should this request for expedition be granted. These documents should be at Defendants' and non-party service providers' easy disposal, and they will suffer little if any "injury" from having to produce the sought-after information sooner rather than later. Conversely, without expedition, Cisco and the public will continue to be harmed by each and every additional sale of counterfeit product, and Cisco may—as Congress contemplated—find itself without any evidence to prove its case.

IV. THE COURT SHOULD ORDER ALTERNATIVE SERVICE OF PROCESS

Under Rule 4(f)(3) of the Federal Rules of Civil Procedure, this Court is permitted to authorize service of process "by other means not prohibited by international agreement, as the court orders." "Rule 4(f)(3) is 'just as favored as service available under Rule 4(f)(1) or Rule 4(f)(2),'" and "[t]he district court has sound discretion to determine 'when the particularities and necessities of a given case require alternate service of process under Rule 4(f)(3).'" *Tracfone Wireless, Inc. v. Washington*, 290 F.R.D. 686, 687-88 (M.D. Fla. 2013) (quoting *Rio Props., Inc. v. Rio Int'l Interlink*, 284 F.3d 1007, 1015-16 (9th Cir. 2002)). "In fact, the validity of electronic service of process upon foreign defendants has been recognized since as long ago as 1980." *Microsoft Corp. v. Doe*, 2012 U.S. Dist. LEXIS 162122, at *6 (E.D.N.Y. Nov. 13, 2012).

In circumstances such as these, where the Defendants are involved in the illegal distribution and sale of counterfeit products are foreign internet-based businesses located in China, and will likely attempt to evade service, courts have readily granted alternative methods of service of the summons and complaint, including by email. *See, e.g.*, *id.*; (approving of plaintiffs' email and internet-based service of process upon anonymous defendants); *FTC v. PCCare247 Inc.*, 2013 U.S. Dist. LEXIS 31969, at *18 (S.D.N.Y. Mar. 7, 2013) (authorizing

service by email and Facebook upon individuals in India responsible for fraud on American citizens); *Carson v. Griffin*, 2013 U.S. Dist. LEXIS 77087, at *5 (N.D. Cal. May 31, 2013) (authorizing service by email for resident of Dubai); *see also Lexmark Int'l, Inc. v. Ink Techs. Printer Supplies, LLC*, 295 F.R.D. 259, 262 (S.D. Ohio 2013) (authorizing service by email to defendants in China and Poland); *Jenkins v. Pooke*, 2009 U.S. Dist. LEXIS 18975, at *6 (N.D. Cal. Feb. 17, 2009) (authorizing service by email to defendant in Great Britain). *See generally WeWork Cos. v. WePlus (Shanghai) Tech. Co.*, 2019 U.S. Dist. LEXIS 5047, at *6 (N.D. Cal. Jan. 10, 2019) (collecting cases). Cisco need not show that other, more traditional means of service were unsuccessful. *See AMTO, LLC v. Bedford Asset Mgmt., LLC*, 2015 U.S. Dist. LEXIS 70577, at *11-12 (S.D.N.Y. June 1, 2015) ("Service of process under Rule 4(f)(3) is neither a last resort nor extraordinary relief.… [A] plaintiff is *not* required to attempt service through the other provisions of Rule 4(f) before the Court may order service pursuant to Rule 4(f)(3)." (internal quotation marks and citation omitted)); *see, e.g.*, *Elsevier, Inc. v. Siew Yee Chew*, 287 F. Supp. 3d 374, 377-78 (S.D.N.Y. 2018) (allowing email service on Chinese and Malaysian defendants without requiring plaintiff to first show that other methods were unavailable or unsuccessful) (collecting cases).

Therefore, Cisco requests that the Court authorize service of the summons and complaint in this action as follows:

- via email on the Defendant Shenzhen Tianheng at the email address it used to communicate with and that was listed on the invoices it sent to Cisco's undercover investigator: thofly@live.com (*see* Vogel Decl. ¶¶ 7-8; *see also* White Decl., Schedule A)

- via email on the Shenzhen Sourcelight Defendants at the email address they used to communicate with and that was listed on the invoices it sent to Cisco's undercover investigator: ayu@sourcelight.com.cn (*see* Vogel Decl. ¶¶ 23-26; *see also* White Decl., Schedule A)
- via email on Defendant Gezhi Photonics at the email address it used to communicate with Cisco's undercover investigator: ena@gezhiphotonics.com (*see* Vogel Decl. ¶¶ 15-16; *see also* White Decl., Schedule A)

V. A BOND IS NOT NECESSARY TO SECURE THE INJUNCTIVE RELIEF

Federal Rule of Civil Procedure 65(c) gives the district court wide discretion to set the amount of a bond or to dispense with the requirement of a bond, in issuing preliminary injunctive relief. *See Doctor's Assocs. v. Distajo*, 107 F.3d 126, 136 (2d Cir. 1996). Because of the strong and unequivocal nature of Cisco's evidence of counterfeiting, infringement, and unfair competition, Cisco respectfully requests that this Court dispense with the filing of a bond. In the event, however, the Court determines that a bond is appropriate, a bond of no more than ten thousand U.S. dollars ($10,000) would be sufficient. *See, e.g.*, *Deckers Outdoor Corp.*, No. 15-cv-3249 (N.D. Ill. Apr. 24, 2015) (ordering a $10,000 bond).

CONCLUSION

Defendants' counterfeiting operations are irreparably harming Cisco's business, its famous brand, American consumers, and America's informational infrastructure. Without entry of the requested relief, Defendants' sale of counterfeit Cisco transceivers will continue to lead purchasers to believe that Defendants' counterfeit transceivers have been manufactured by or emanate from Cisco, when in fact they have not. The Court should grant Cisco's Order To Show Cause for a temporary restraining order, an *ex parte* asset freeze order, expedited discovery, an

order permitting alternative service, and a preliminary injunction, and should award any other and further relief that the Court deems just and proper.

DATED: November 22, 2019
New York, New York

Respectfully submitted,

/s/ Geoffrey Potter

Geoffrey Potter
R. James Madigan III
PATTERSON BELKNAP WEBB & TYLER LLP
1133 Avenue of the Americas
New York, NY 10036-6710
Telephone: (212) 336-2000
Fax: (212) 336-2222
gpotter@pbwt.com
jmadigan@pbwt.com

Attorneys for Plaintiffs Cisco Systems, Inc. and Cisco Technology, Inc.